APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
08/994,878	12/19/97	EPSTEIN	M	PHA-23.313

LM02/1005

JACK E HAKEN
US PHILIPS CORP
INTELLECTUAL PROP DEPT
580 WHITE PLAINS ROAD
TARRYTOWN NY 10591

	EXAMINER
	SONG,H

ART UNIT	PAPER NUMBER
2766	5

DATE MAILED:
10/05/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

☒ Responsive to communication(s) filed on _Dec 19, 1997_ .

☐ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire ____3____ month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) _1-20_ is/are pending in the application.

   Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) _1-20_ is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☒ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐approved ☐disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

   ☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

      ☐ received.

      ☐ received in Application No. (Series Code/Serial Number) _____ .

      ☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   *Certified copies not received: _____ .

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). _3,4_

☐ Interview Summary, PTO-413

☒ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

Claim Objections

1.   Claim 11 is objected to because of the following informalities: in line 2, "`:`" is missing after

the word comprising. "Computer readable storage means" should start in a new line Appropriate

correction is required.

Claim Rejections - 35 USC § 103

2   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3   Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dolan(US

5,604,801) in view of Krajewski(US 5,590,199).

In claims 1-4, Dolan discloses receiving via the network a user's ID in (fig.5). Reading

from a storage means data corresponding to the user having the received ID, which data

comprises the user's private key encrypted using a key determined from identifying information of

the user in (abstract, lines 7-12,col.3, lines 5-11). Dolan does not discloses sending via the

network the encrypted private key, whereby the encrypted private key can be received and

decrypted at the location of the user using the user's identifying information. Krajewski discloses

where user receives and decrypts the encrypted key at user's site using a user's identifying

information in (col.6, lines 18-35). It would have been obvious to a person of ordinary skill in the

art at the time the invention was made to use Krajewski's method where decryption is done in

user's site with Dolan because the user does not have to transmit sensitive information such as

biometric information where it is prone to data interception by the hackers. Security of the data is

greatly enhanced by keeping the data at user's site rather than transmitting it over the network.

Claim 5 different from claim 1 in that private key is destroyed at the location of the user.

Dolan discloses deleting a private key after use in (abstract, lines 15-16,fig.4(b)#495).

In claim 6, Dolan discloses user entering a password in (fig.5). The examiner asserts that

password can be an another form of passphrase or biometric information.

In claims 7-10, computing a hash document and encrypting the hash using the user's

private key and transmitting the encrypted hash is disclosed by Dolan in (col.6, lines 1-15).

4.   Claims 11-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dolan.

In claim 11, Dolan discloses respective IDs and encrypted private keys are stored in the

storage in (col.3, lines 4-10). Dolan does not specifically discloses private key is encrypted with

uer identifying information. However, Dolan discloses private key is enrypted with a key

encrypting key. The examiner asserts that since user has the key encrypting key, it can be a user

identifying information.

In claim 12, see claim rejection 6 above.

In claims 13-14, Dolan discloses hash function and random number stored in the storage in

(fig.2, col.4, lines 20-24).

In claims 15-16,19, see claim rejection 1 above.

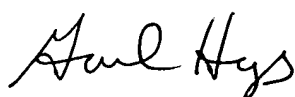In claims 17-18, see claim rejection 7-10 above.

In claim 20, Dolan discloses user terminal interconnected via a network to the server in

(fig.1). Dolan discloses user terminal is configured for transmitting to the server via the network

an ID entered by the user in (fig.5). Receiving and decrypting an encrypted private key received

via the network from the server using a user identifying key determined from a passphrase entered

by the user or biometric information obtained by measuring the user is discussed in claims

rejection 1-4 above.

5.   Any inquiry concerning this communication should be directed to Ho S. Song at telephone

number (703)305-0042. The examiner can normally be reached on Monday through Friday from

7:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gail Hayes, can be reached at (703)305-9711.

Any inquiry of a general nature or relating to the status of this application or preceeding

should be directed to the group receptionist, whose telephone number is (703)305-3800.

Ho Song

GAIL O. HAYES
SUPERVISORY PATENT EXAMINER
GROUP 2700